EAI Endorsed Transactions
on Security and Safety

Research Article EAI.EU

A study of user experiences and network analysis on anonymity and traceability of bitcoin transactions

M A Hannan Bin Azhar[1,*] and Robert Vause Whitehead[1]

[1]School of Engineering, Technology and Design, Canterbury Christ Church University, UK.

Abstract

This paper investigates the anonymity of bitcoin transactions and significance of awareness of the technology by bitcoin users, alongside their experiences in tracing transactions. Bitcoin enables users to carry out transactions anonymously with the virtual currency without unveiling where the real-world source of the income has come from. These transactions may occur without revealing locations or any personal identifiable information of the person who is sending or receiving bitcoins. While there are existing surveys which test bitcoin users' awareness of the technology, they do not focus on bitcoin users' own experience using the technology in terms of tracing transactions and use of anti-forensic tools to increase the level of anonymity. This paper reports significance of users' opinions on traceability and anonymity of bitcoin transactions and compares users' viewpoints collected from a survey with experimental findings observed using network analysis tools.

Keywords: Bitcoin, Blockchain, Crypto-currency, Digital Currency, Privacy, Security.

Received on 01 April 2021, accepted on 30 April 2021, published on 30 April 2021

doi: 10.4108/eai.30-4-2021.169577

1. Introduction

Bitcoin offers its users a virtual currency which can be transferred to any bitcoin wallet in the world with little effort and small transfer fees. It allows users to do it with anonymity [1]. Bitcoin wallets and some bitcoin exchanges do not require identifiable information to use them. A bitcoin user does not explicitly require personal identifiable information to perform transactions [2]. What makes Bitcoin anonymous is the lack of accompaniment between the public key and any requirements of identity data [3]. As a result, these functions give Bitcoin its anonymous element. There is a debate that Bitcoin may not be completely anonymous, such cases of accidental disclosure of a person's public key or even voluntary disclosure links identity data with a public key [2]. There is also the choice for bitcoin users to use anti-forensic tools to increase their anonymity. The introduction of "mixing services" or dark wallets allow for multiple people to contribute to a movement of bitcoins, which can expertly disguise a transaction by mixing it with other transactions, and then sending that "mixed" transaction at a different time within that day [4]. This stops analysis being done on the time and amount that was sent on a transaction. In addition to mixing services, the use of a virtual private network (VPN) and a Tor type browser makes it more difficult to track a transaction [1], although it does not make it impossible or a momentous barrier to tracing transactions.

While there are surveys [5][6] which test bitcoin users' awareness of the technology, they do not focus on bitcoin users' own experience using the technology in terms of tracing transactions and use of anti-forensic tools. The survey is used to assist in monitoring bitcoin users' awareness of the main concerns that come with using bitcoin, as well as finding statistical data on the bitcoin users' experience levels and success with tracing transactions. This paper will compare results of the survey with experimental findings using network analysis. Subjective opinions collected from the survey and objective measures from experiments will be compared to

*Corresponding author. Email: hannan.azhar@canterbury.ac.uk

report findings on traceability and anonymity of bitcoin transactions.

The remainder of the paper will be organised as follows: Section 2 discusses the crime reported in relation to bitcoins and the existing literature surrounding the traceability of bitcoin transactions. Methodological approaches for the experiments and survey design are detailed in Section 3. Section 4 presents the experimental results and analysis from the survey. Finally, Section 5 concludes the paper.

2. Literature review

Literature review will discuss what already has been reported on bitcoin crimes, traceability of bitcoin using tools, laws and regulations related to bitcoins and findings from surveys in relation to users' opinions on anonymity and traceability of bitcoins.

2.1. Bitcoin related crimes

Prior studies have identified a link with bitcoin and criminal activity. Reference [7] reports a number of high-profile investigations into the organised crimes and suggests that bitcoins are becoming the currency of choice for many criminals. Money laundering, transferring of funds between bad actors and payment for illegal services have all been reported as practices used by criminals in hand with bitcoins [8]. An FBI report on Bitcoin anticipates seeing increased Bitcoin money laundering activities [9]. Criminals have been found to exhibit increased interest in using cryptocurrency to launder money and fund their illicit activities. The same report depicts the challenges that FBI might face in the future for deterring illicit activity that comes with the use of Bitcoin by criminals, revealing that Bitcoin could become a frequent payment method used by bad actors, and could be used to fund their illegal activities. In November 2015, a computer hacktivist group known as Ghost Security Group claimed to locate Bitcoin wallets that were used by ISIS. They disclosed that there was between $4.7m and $15.7m within ISIS Bitcoin wallets, these figures were shown to represent between one to three per cent of ISIS annual income within 2015 [10]. There is evidence that Bitcoin has already been used to fund terrorism. It was reported that in 2015 in Jakarta, a terrorist with the knowledge of cryptocurrency was inspired by ISIS and demanded bitcoins from the owners of a shopping mall, where he had planted a bomb in [11]. Although there is no guarantee that Bitcoin will be used as a major source for funding terrorist groups and other criminals, it is likely that the cryptocurrency medium used by bad actors will only increase.

2.2. Traceability of bitcoin

Hiding personal identifiable information (PII) on the internet is a difficult task, as quite often a person can leave a digital footprint of his or her online activity. The method of tracking users through IP addresses is limited considering that a bad actor could implement technology such as TOR or a VPN to cloak their activities [1]. Reference [12] highlights methods which could be used to trace bitcoin transactions, but criticizes aspects of the tracing process, questioning that linking pseudonyms to an address during analysis is circumstantial, stating that the "trail is noisy and deniable". In Ref. [13], experiments were conducted to test how bitcoin transactions work, how the bitcoin protocol operates over the network and what bitcoin artefact can be examined from a digital forensic perspective. The results showed that while tools like Wireshark, Blockchain.info and a bitcoin client can be used to trace potentially illicit financial transactions through the bitcoin blockchain, tracing pseudonymous bitcoin addresses (addresses that may be linked to an online pseudonym or verified account on social media) did not yield PII. Other approaches to tracing transaction come through the form of using the 'Sybil' method of attack, which can potentially be used to map IP addresses to public keys of users [14]. Although this method may not be one-hundred percent accurate unless insignificant pairings are eliminated. Bitcoin users are generally encouraged to create a new bitcoin address for every transaction, which if implemented will decrease the times allowing for patterning of parings and reduce the likelihood of associating PII with bitcoin addresses [15]. In conclusion, there are methods that trace transactions and links actors with their PII, the dilemma is that they do not guarantee success due to actors clouding the trace by using pseudonyms linked with bitcoin addresses, irregular timings of transactions and software which can obfuscate the tracing process. Bitcoins platform is based on anonymity making the tracing process a problematic task, in most cases it relies on the actor "slipping up" and revealing an aspect of their bitcoin addresses.

2.3. Surveys on bitcoin

A survey carried in [5] obtained measurements on the use of digital currency in Canada using an omnibus method. Their findings marked out certain categories within the population on usage, awareness and adoption rates. Similarly, other surveys put forward questions on the security and regulations of cryptocurrencies, asking their participants how they approach security issues of their own personal transactions using virtual currencies, or how they would prefer regulations to be handled on cryptocurrencies. Survey conducted by the IEEE [6] was put out to participants in the wake of bitcoin technology grabbing attention of government bodies due to the increase of malicious actors using it to bypass legal controls. Seemingly, the survey designs being used for the topic of cryptocurrencies bolstered simple questions such as "Have you heard of Bitcoin" with a YES or NO answer, focusing on descriptive statistics. Participant pools on the two surveys [5][6] ranged in thousands but did report on

considering that they anticipated a smaller sample of Bitcoin users.

2.4. Regulations & Law on Cryptocurrencies

Every country has their own approach to regulating cryptocurrencies. Reference [16] classifies countries' approaches to cryptocurrencies in six levels (0-5), which rates the state's attitudes towards cryptocurrencies. The UK government is undertaking research as to how it should respond to cryptocurrency. A report released by the UK government's chief scientific advisor concluded that governments should regulate ledger systems like Bitcoin by influencing the technical code that defines their rules; saying that, policymakers should recognise the influence of technical code and advise it to be made part of the regulatory system [17]. Even if the technical code was influenced by governmental bodies, what might be the purpose of doing so? Another article [18] implies that nations are trying to seek influence over cryptocurrencies. China for instance is dominant for mining cryptocurrencies internationally. Questions could be asked, if cryptocurrencies become widely embraced, who will have the main authority of the currencies? Will they stay decentralised or become centralised ledgers under governmental control and use to manipulate the financial system [18]. Regulations on Bitcoin are either minimal or heavy depending on the country the user operates within. Countries such as Egypt, Bolivia, Nepal, Morocco and Algeria all have a complete ban on cryptocurrency transactions [16]. What may eventually occur if virtual currencies do become widely adopted is that the country which has dominancy within cryptocurrency infrastructure may eventually take the majority control of the market. At the same time, if governmental control is applied in the form of influence over the technical code, the effects on the use of cryptocurrencies are unknown.

In conclusions, literature review examines the main discussion points of Bitcoin, highlighting the main agreements and disagreements in current literature. The discussions surrounding methods of traceability seem to be flawless in having the same conclusion of findings that the tracing process is complicated and does not always yield results. Most journals covering the subject test traceability under the parameters of network analysis, querying the Blockchain for information and verification of transactions. This may be down to the research found on the cryptography used by Bitcoin, as it is currently impenetrable with no algorithm in existence to break the encryption it uses. The literature on surveys was especially found to be important as it is the centre of knowing the consensus of bitcoin users' awareness of the technology. Further research and surveys are required to gain a better understanding of how the process of tracing a transaction via network analysis may lead to showing information, which could link a packet using the Bitcoin protocol back to personal identifiable information.

3. Methodology

The experimental research reported in this paper draws upon some of the methodology used in previous literature, such as in [13] [15] [19], in the attempt to trace a transaction and de-anonymise the actor through the means of analysing network activity. However, the other focus of the study surrounds bitcoin users' opinions on methods of tracing transactions and their own use of tools to increase anonymity of Bitcoin transactions.

3.1. Tools used

To uncover traces on transaction a number of tools were used. For the tracing process: Exodus, blockchain.info, Wireshark, Tunnelbear and Maltego were used. Exodus is a top-rate desktop and mobile wallet for multiple digital currencies, allowing users to send and receive digital currencies. It is very easy to use with an intuitive graphical user interface (GUI), as shown in Fig. 1. It was picked over bitcoin core, which is considered bitcoin reference implementation. Unlike the core, it does not require the full 200+ GB download of the whole bitcoin blockchain, which is used to verify payments.

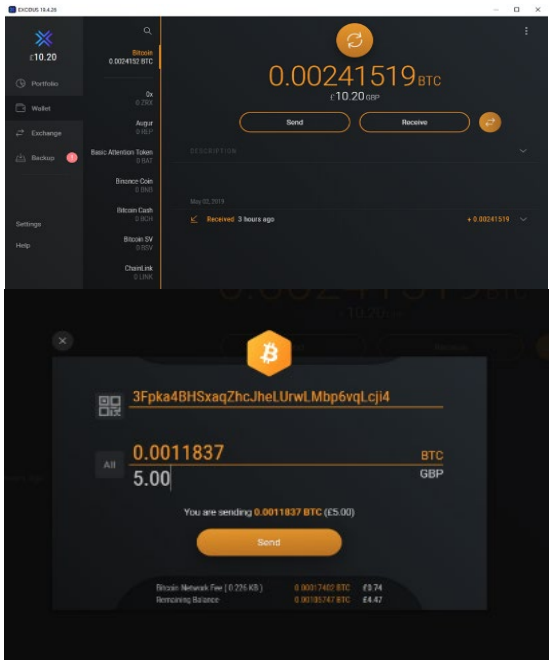

Figure 1. Exodus (Bitcoin wallet menu).

Exodus's main menu of the bitcoin wallet presents a screen that allows users to send or request funds. Figure 1 shows that the funds are being prepared to be sent to a bitcoin address. To verify the transaction occurred, the website blockchain.info was used to query if the funds were taken out of the sending address and sent to the receiving address. Figure 2 presents the number of

transactions that have occurred on the address (no. transactions: 1), the amount of bitcoin received, the balance (0.0011837 BTC) and most importantly the transaction history, which in this case does verify the addresses and the amount that was sent except the fees.

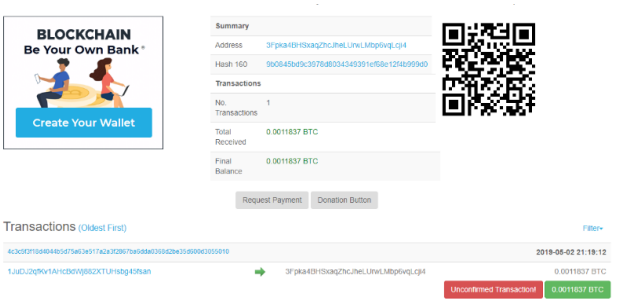

Figure 2. Blockchain.info verifying that the transaction occurred.

Maltego is a visual link analysis tool, which uses plugin called "transforms". This tool offers information gathering and represents any information using a node-based graph. In the event that a bitcoin address or transaction code is found, Maltego can be used to visualise the transaction and mine information related to the address, it can then be used to scan websites for information related to an address which may lead to personal identifiable information of a bitcoin user.

TunnelBear, a secure VPN service, was launched at the beginning of the experiment, to bypass the geographic location and to see if the use of this tool can be used as anti-forensic software to restrict the transaction from being traced. The location of TunnelBear was set as Japan. Japan's law on Bitcoin and cryptocurrencies are not as restricted in comparison to other countries and remains a friendly environment to conduct such experiments on cryptocurrencies; using Japan as the geographic location does not go against their laws [20].

While using VPN, another payment was sent to a bitcoin address, with a different amount of currency (0.00089608 BTC) being sent to differentiate from the previous payment. Blockchain.info was used again to verify the funds were received from the Bitcoin wallet address stored by Exodus. The number of transactions was one and the amount sent was 0.00089608 BTC, which correlates to the amount minus fees sent to the address. Exodus transaction history also verified that the transaction was sent.

Wireshark offers its users a platform to carry out a deep inspection of hundreds of protocols, including offering of a bitcoin dissector to analyse the bitcoin protocol. During the analysis of what tools to use, Wireshark seemed to be the distinct option in comparison to other packet sniffing tools due to the features it offers its users. In comparison to other tools, such as SmartSniff or Microsoft Message Analyser, Wireshark came across as the superior option due to its features and easy to use GUI.

3.2. Survey design

The survey was created and hosted by google forms, which offers the user the ability to download all the data for a more in-depth analysis using statistical software like SPSS. SPSS offers a comprehensive set of statistical tools which are easy to use when generating statistical analysis from the data. The survey consists of fourteen questions asking from demographic information to more detailed descriptive questions. The table below specifies the questions used, as well as the justification for using such questions.

Table 1. Survey questions

Questions	Justifications
What is your age?	Asking the participant's age was used to see if a certain category of age is more likely to be invested in using Bitcoin technology.
What is your gender?	To see if there is a higher division of a certain gender that is more likely to use Bitcoin.
What is the highest level of education you have completed?	Analysing for clear demographic to a category of completed education and a link towards Bitcoin experience.
What area do you work or study in?	To gather information of the socio-economic status the user is in.
What level of experience have you had in using bitcoin?	To explore if there is a correlation between experience level with other information such as tracing success rate, use of anti-forensic software etc.
How important are these factors as advantages for bitcoin?	Enquiring about the participants' opinions on certain features that come along with using bitcoin technology, to test if there is a pattern towards people's viewpoints on these features.
Have you ever tracked/traced a bitcoin transaction?	To gather user experience on traceability
Which methods have/would you use to trace a bitcoin transaction?	To investigate traceability success specific to methods used.
Do you believe the use of bitcoin dissectors used by packet sniffers are a good option for network analysis?	The method of using network analysis tools are common in the industry for cyber security. The bitcoin protocol is not always covered by these technologies, implementing bitcoin dissectors into network analysis tools is asked to participants to gain their viewpoints on the use of these within the software.
Do you agree with the use of chain-analysis to track transaction?	Chain analysis is a new tool for forensic investigation on cryptocurrencies. These tools have been proven to help on investigations related to cryptocurrencies. The participant is

Questions	Justifications
	asked on their opinions on the use of this technology, analysis of which will be carried out if significant results are found.
What was your success rate in tracking/tracing the transactions?	To investigate if there is a higher increase of success through using a specific tool.
Have you used software to increase the anonymity of your transactions?	To get an estimate on the number of users that try to increase their anonymity. It is an important statistic to know, it may impact the results of tracing their transactions. Software such as VPNs, PGP encryption and Wallet Mixing services are listed as options for choices. They can select more than one software if they have used multiple applications.
Has this affected the traceability of your own transactions using software to increase your anonymity?	Is there a correlation between using the previous questions tools and increasing the success rate of tracing a transaction?

The number of participants in the survey was 27. Ethical approval was obtained, and participants gave consent to take part in the study. The survey was handed out only to the associates who have had previous experience with Bitcoin and was also posted out to bitcoin community via bitcoin forums. Participants ranged in their experiences of using bitcoins from a beginner at the entry level of sending and receiving transactions to participants who were proficient using bitcoins.

4. Results and discussion

Results cover the key findings from the analysis described in the previous section. Results are presented with regards to two categories: traceability using tools and survey results.

4.1. Traceability of bitcoins using tools

Figure 3 shows the Wireshark analysis on the bitcoin packets those were captured during the time of the transactions. There was a huge amount of data to surf through on the initial analysis, but previous literature [19] made it clear that the bitcoin packets containing the 'TX' information would be the place to start the investigation. Any unspent coins or "unspent transaction outputs" (UTXO), which have a certain denomination and an owner defined by the 20-byte address generated as a bitcoin address, are assigned to the user.

Bitcoin transactions work on TX functions in relation to the protocol, which require a signature when initialized, if the signature does not match the owner of the UTXO, it will return an error. If the signature is correct, the UTXO is removed from the address and output to the receiver's address (after going through the mining process). Figure 3 shows Wireshark logs depicting the information it received about the transactions via the TX info.

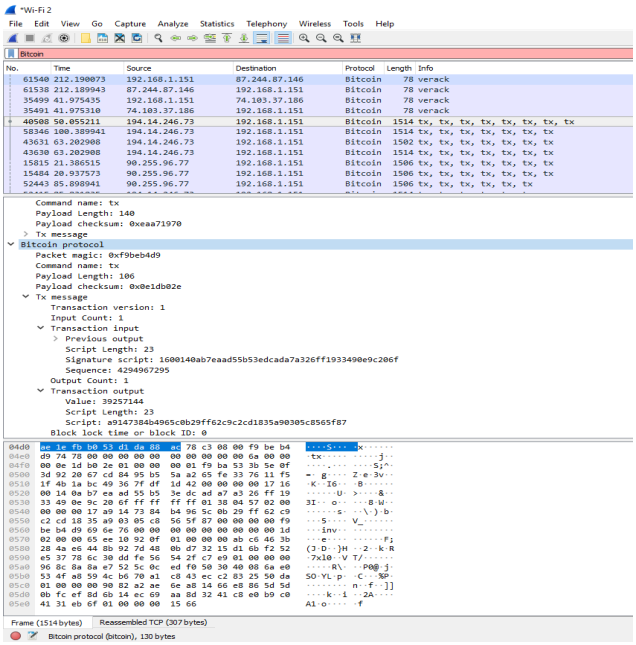

Figure 3. Wireshark analysis on the bitcoin packets.

Table 2. Wireshark logs

Field Size	Description	Comments
1+	Input count	The number of transactions inputted
1+	Script Length	The length of the signature script (This is the signature that needs to be authorized so the funds can be sent.)
N/A	Signature script	The script for confirming transaction authorization.
4	Sequence	Transaction version which is defined by the sender. This creates details of the transaction before being included into a block.

Table 2 lists some of the key information that can be gathered from the transaction. These four fields indicate how many transactions took place, the length of the signature and the signature script and the sequence, which is all relative information connected to the sender. The problem with this information was that it did not reveal any PII. However, the results of the information can be useful for further investigations, such as knowing the amount of transactions that took place and the signature can be critical to linking a suspect to evidence of the transaction. The signature cannot link back to PII because inherently it is

generated from a hash (of something that has to be signed) plus the private key. The private key goes through the process of the elliptic curve digital signature [21] algorithm to mask its identity. The elliptic curve digital signature algorithm at this point in time has no algorithm to crack it with [21].

Figure 4. Blockchain.info verifying the transaction.

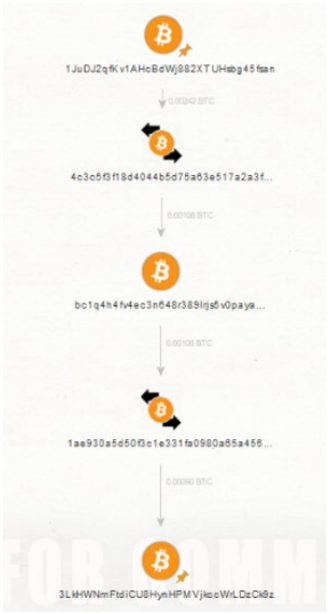

Figure 5. Maltego created visual node diagram.

The use of a VPN did not mask the discovery of the bitcoin protocol being found over the network using Wireshark, and also TX information did not lead to the discovery of any personal identification information. All attempts with TunnelBear failed to hide the discovery of the protocol. Nonetheless, when verifying blockchain.info on the transaction that occurred with VPN, the results show the payment did not go to the originally addressed input (Fig. 4). When investigating the cause of this using Maltego (Fig. 5), which creates a visual node diagram of the bitcoin address and transactions, it was found that the fee for mining the block containing this transaction was sent to an address before the amount without the fees was sent to the correct bitcoin address.

4.2. Survey analysis

Survey was conducted amongst participants of bitcoin users from varied experience level. They were representative of wide range of professions and studies from both STEM (Science, technology, engineering, and mathematics) and non-STEM background. Survey results showed difference between males and females that were in the STEM or Non-STEM areas of works and studies. Majority of the participants (70%) were aged 18-25. It was found that males were likely to be STEM orientated areas of work in comparison to females who were likely to be in Non-STEM areas of work as seen in Fig. 6. Amongst the participants those reported some level of success in tracing bitcoins, STEM related participants had a higher rate of success in comparison to Non-STEM users. This has been illustrated in Fig. 7.

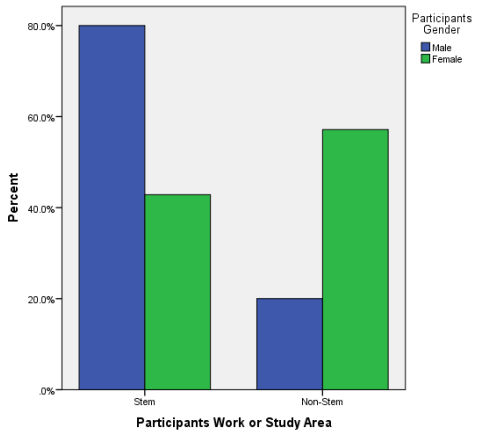

Figure 6. STEM and Non-STEM Gender.

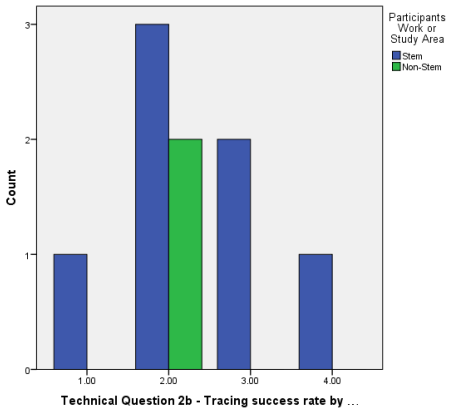

Figure 7. Success in tracing bitcoin.

There were statistically significant correlations on participants' opinions on the governance for bitcoin transactions with anonymity and traceability as a disadvantage to bitcoin transactions. Participants viewed in favour of central control for bitcoin transactions, also viewed strongly that transactions should be anonymous and not traceable. A Spearman's correlation was run to determine the relationship between participants' views on governance and anonymity and traceability as a disadvantage to bitcoin transactions. There was a strong, positive monotonic correlation observed ($r=.624$, $n=27$, $p<.0001$).

Amongst the half of the participants who reported use of tools in tracing bitcoins, 69.2% used only heuristic method, while 15.4% used only packet sniffing software. Packet sniffing tools can be used while a user is on a network and interacting with any cryptocurrency. Depending on the bitcoin protocol used, it may limit what data can be received. Heuristic method on the other hand can give evidence on users if they are not careful enough to hide their identity. For example, bitcoin addresses of a user found on a forum or media channel can be linked to a criminal activity and this can be used as an evidence to prosecute a suspect in the court.

Figure 8. Tracing success.

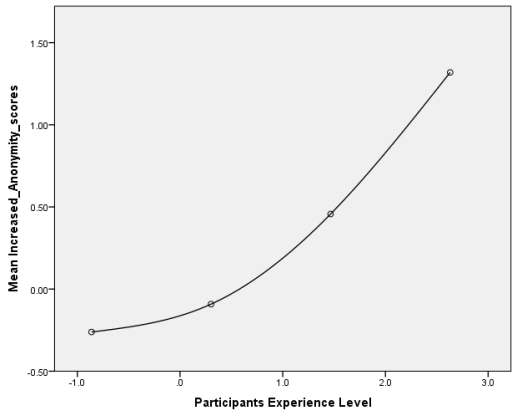

Figure 9. Increased anonymity.

It was also observed that participants who believed they had higher level of experience in using bitcoins, were more successful in tracing bit coin transactions. Pearson's score for participants views on their experience level in using bitcoins and their ratings of success in tracing bit coin transactions was statistically significant ($r=.383$, $p<.05$), also regression analysis showed statistically significant positive linear relationship ($r2=0.147$, $p<0.05$) as shown in the Fig. 8. The mean plot of Fig. 9 suggests that there was a positive correlation between participants experience level and success rate on anonymity with anti-forensics tools, but the relationship was not statistically significant ($r=.343$, $p=.12$).

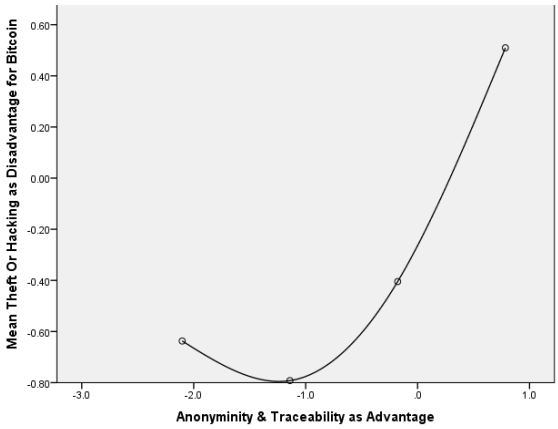

Figure 10. Mean plot of Theft and hacking with anonymity and traceability.

The mean plot in Figure 10 shows users who ranked higher for importance on anonymity & traceability as advantage also ranked higher for importance on theft or hacking as a disadvantage for bitcoins. While bitcoins are preferred to be traceable and being anonymous, international transactions are favourable; participants' views on this were statistically significant ($r=0.43$, $p=0.02$).

4. Conclusions

The design philosophy of Bitcoin shows how intricate it is to allow a trace on locating data on a specific user with the adoption of network analysis. On the other hand, the information from the survey results shows that Bitcoin users tend to have similar experiences. Survey was representative to the samples and responses captured bitcoin users' own experience using the technology in terms of tracing transactions and use of anti-forensic tools. Several statistical significant results were found from users' opinions. Statistically significant relationship was found between self-rated positive attitude towards anonymity & traceability and self-rated negative attitude towards theft and hacking for bitcoin. Relationship between participants' views on governance and anonymity and traceability as a disadvantage to bitcoin transactions was statistically significant. Statistical analysis shows that the users who used combination of at least two anti-forensic tools were in favour of their increase of anonymity compared to the groups who did not use any tool at all. The large majority of users do not have success in tracing transactions. Network analysis could not lead to uncovering personal identification number and this may be down to the infrastructure of Bitcoin and how integral it is to keep a user anonymous.

Bitcoin users already have a high degree of anonymity while using the technology, which is only increased if they incorporate software such as VPN and bitcoin mixing services. Although Wireshark did not disclose any personal identification information over the Bitcoin protocol, it did display source/destination IP addresses, which would be useful information to have within an organisation, in tracing who sent or received the virtual currency over the network. This might entail further investigation into how they managed to do so (if against policy to do so), or if certain tools are being used to disguise the transactions. While there are tools to create visual diagrams and use big data analysis to find evidence of the identity of Bitcoin users, they are not yet readily available to the public. During the initial phase of researching the tools available for this purpose, Maltego was the only option that was easily available. Although, creating a database of known bitcoin users linked to addresses may be a useful tool, it requires further investigation into the feasibility of its usefulness. Crypto forensics companies like CypherTrace have already started this process of monitoring transactions for unusual payment times and amounts, while investigating where these payments are going to or linking to certain criminal organisations evading anti-money laundering or involved in activities like terrorist financing.

References

[1] Reynolds, P. and Irwin, A. (2017). Tracking digital footprints: anonymity within the bitcoin system. Journal of Money Laundering Control, 20(2), pp.172-189.

[2] Taylor, M. (2019). Bitcoin and the Age of Bespoke Silicon. [online] pp.pg.1-10. Available at: https://allquantor.at/blockchainbib/pdf/taylor2013bitcoin.pdf [Accessed 31/3/2021].

[3] Dion, D. (2013). I'll gladly trade you two bits on Tuesday for a byte today: Bitcoin, regulating fraud in the E-conomy of hacker-cash. [online] Illinoisjltp.com. Available at: http://illinoisjltp.com/journal/wp-content/uploads/2013/05/Dion.pdf [Accessed 31/3/2021].

[4] ShenTu, Q. and Yu, J. (2019). Transaction Remote Release (TRR): A New Anonymization Technology for Bitcoin. ATR Defense Science & Technology Lab., Shenzhen University, Shenzhen, China, [online] pp.pg.1-18. Available at: https://pdfs.semanticscholar.org/1fa5/2a38df75618b7370dcf6b92eeec896a86fc8.pdf [Accessed 31/3/2021].

[5] Henry, C., Huynh, K. and Nicholls, G. (2019). Bitcoin Awareness and Usage in Canada: An Update. The Journal of Investing, [online] 28(3), pp.21-31. Available at: https://www.bankofcanada.ca/wp-content/uploads/2017/12/swp2017-56.pdf.

[6] Conti, M., Sandeep Kumar, E., Lal, C. and Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys & Tutorials, 20(4), pp.3416-3452.

[7] Angela S.M. Irwin, George Milad, (2016) "The use of crypto-currencies in funding violent jihad", Journal of Money Laundering Control, Vol. 19 Issue: 4, pp.407-425, https://doi.org/10.1108/JMLC-01-2016-0003.

[8] Oxford Law Faculty. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?. [online] Available at: https://www.law.ox.ac.uk/business-law-blog/blog/2018/02/sex-drugs-and-bitcoin-how-much-illegal-activity-financed-through [Accessed 31/3/2021].

[9] FBI (2012). Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity. [online] Available at: https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf [Accessed 31/3/2021].

[10] Estrada, M., Siegal, J. and Estrada, M. (2019). ISIS parks its cash in Bitcoin, experts say. [online] BGR. Available at: https://bgr.com/2015/11/25/isis-parks-its-cash-in-bitcoin-experts-say/ [Accessed 31/3/2021].

[11] Pick, L. (2015). Jakarta "Toilet Bomber" Demanded 100 Bitcoins, Inspired by ISIS | Finance Magnates. [online] Finance Magnates | Financial and business news. Available at: https://www.financemagnates.com/cryptocurrency/news/jakarta-toilet-bomber-demanded-100-bitcoins-inspired-by-isis/ [Accessed 31/3/2021].

[12] Kaminsky, D. (2011). Black Ops of TCP/IP 2011. [online] Dan Kaminsky's Blog. Available at: https://dankaminsky.com/2011/08/05/bo2k11/ [Accessed 31/3/2021].

[13] Turner, A. and Irwin, A. (2018). Bitcoin transactions: a digital discovery of illicit activity on the blockchain. Journal of Financial Crime, 25(1), pp.109-130.

[14] ShenTu, Q. and Yu, J. (2019). Transaction Remote Release (TRR): A New Anonymization Technology for Bitcoin. ATR Defense Science & Technology Lab., Shenzhen University, Shenzhen, China, [online] pp.pg.1-18.

[15] Koshy, P., Koshy, D. and McDaniel, P. (2014). An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. Pennsylvania State University. [online] Available at: http://fc14.ifca.ai/papers/fc14_submission_71.pdf [Accessed 31/3/2021].

[16] Lansky, J. (2018). Possible State Approaches to Cryptocurrencies. Journal of Systems Integration, 9(1), pp.19-31.

[17] Government Office for Science (2016). Distributed Ledger Technology: beyond block chain. [online] Government Office for Science, pp.p.1-88. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf [Accessed 31/3/2021].

[18] Robinson, D. (2019). The Implications of Cryptocurrency Exploitation by Nation-States. [online], Available at: https://www.elliptic.co/our-thinking/cryptocurrency-exploitation-nation-states [Accessed 31/3/2021].

[19] Hamid Lone, A. and Naaz Mir, R. (2018). Investigating and Analyzing Bitcoin Blockchain Protocol using Wireshark. International Journal of Computer Network and Information Security, 10(7), pp.36-43.

[20] ComplyAdvantage. (2019). Crypto Regulations in Japan. [online] Available at: https://complyadvantage.com/knowledgebase/crypto-regulations/cryptocurrency-regulations-japan/ [Accessed 31/3/2021].

[21] Knutson, H. (2018). What is the math behind elliptic curve cryptography?. [online] Hacker Noon. Available at: https://hackernoon.com/what-is-the-math-behind-elliptic-curve-cryptography-f61b25253da3 [Accessed 31/3/2021].